The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
07/12/2016

SUBJECT:
A Vulnerability in Microsoft Jscript and VBScript Could Allow for Remote Code Execution (MS16-086)

OVERVIEW:
A vulnerability exists in Microsoft Jscript and VBScript engines that could allow for remote code execution if a user visits a specially crafted website. Successful exploitation could result in the attacker gaining the same user rights as the logged on user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE
There are no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:
- VBScript 5.7 on Windows Vista installations using Service Pack 2, Windows Server 2008 installations using Service Pack 2
- Jscript 5.8 and VBScript 5.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core Installation Only)

RISK:
Government:
Large and medium government entities: **High**
Small government entities: **Medium**
Businesses:
Large and medium business entities: **High**
Small business entities: **Medium**
Home users: Low

TECHNICAL SUMMARY:
A memory corruption vulnerability exists in Microsoft JScript and VBScript engines that could allow for remote code execution if a user visits a specially crafted website. This vulnerability exists in the way these scripting engines render when handling objects in memory for Internet Explorer. This vulnerability could corrupt memory in such a way that an attacker could execute remote code in the context of the current user. (CVE-2016-3204)

Successful exploitation could result in the attacker gaining the same user rights as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Apply the principle of Least Privilege to all systems and services.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from untrusted sources.

REFERENCES:

Microsoft:

https://technet.microsoft.com/en-us/library/security/ms16-086.aspx

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3204